

(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
14 March 2002 (14.03.2002)

PCT

(10) International Publication Number
WO 02/21846 A1(51) International Patent Classification⁷: H04N 7/24

[KR/KR]; Seong-won Apt. 2-dong #1301, Uoo-eui-dong 1, Dobong-gu, 142-090 Seoul (KR). LEE, Jung-Su [KR/KR]; Chungwha villa B03 ho, 315-55 Ssangmun 3 dong, Dobong-gu, 132-033 Seoul (KR).

(21) International Application Number: PCT/KR01/01524

(74) Agent: KOREANA PATENT FIRM; Dong-Kyong Bldg., 824-19 Yoksam-dong, Kangnam-ku, 135-080 Seoul (KR).

(22) International Filing Date:
10 September 2001 (10.09.2001)

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(25) Filing Language: English

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European

(26) Publication Language: English

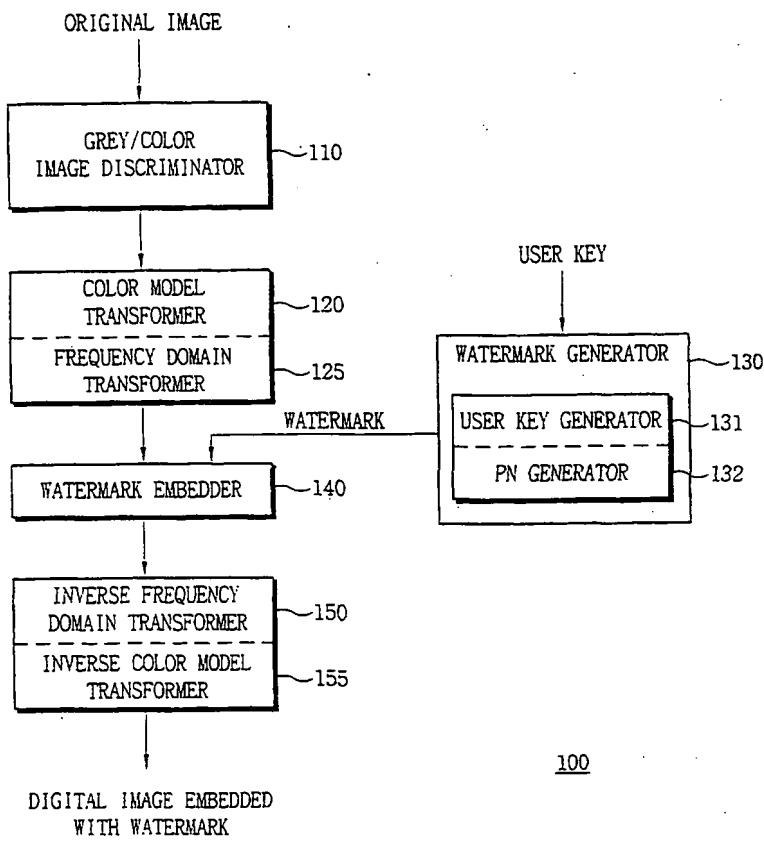
(75) Inventors; and

(76) Inventors/Applicants (for US only): CHOI, Jong-Uk

(77) Abstract: The present invention relates to a digital image watermarking apparatus and method. Luminance component of a digital image are transformed into coefficients of a frequency domain, and watermark is generated by encrypting a user key and generating pseudo random number from encrypted user key. Then, a replacement coefficient generated from a coefficient of a first frequency area and the watermark is replaced with a coefficient of a second frequency area so that the watermark is embedded into the digital image. The embedded watermark is extracted at an authenticating apparatus and the digital image is authenticated by finding the correlation between the extracted watermark and watermark for authentication.

[Continued on next page]

(54) Title: DIGITAL IMAGE WATERMARKING APPARATUS AND METHOD





patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

— entirely in electronic form (except for this front page) and available upon request from the International Bureau

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

- with international search report
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

DIGITAL IMAGE WATERMARKING

APPARATUS AND METHOD

5

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a digital image watermarking apparatus and method, more specifically, which are able to extract the embedded watermark in a good manner and simultaneously do not deteriorate the quality of a digital image and are able to extract the watermark without an original image by strongly remaining a watermark in spite of print or various image alterations.

15 **2. Description of the Related Art**

As creation and distribution of the digital media such a still image as a picture image or such a moving picture as an animation increase, the digital media is circulated through various storage media or network, and thus illegal copy or illegal alteration is largely increased. Various devices have been developed to prevent the digital media from illegally being altered or copied or circulated. As a device for implementing such object, the inventor of the present invention paid attention to a digital watermarking technology.

The digital watermarking technology is to prevent copy, distribution, alternation, sale, etc. without permission of the ownership holder of the digital

data works by additionally embedding information undistinguishable with the naked eye in the digital data works.

There are a spatial domain method, a frequency domain method, a spread spectrum communication method, etc. in the digital watermarking technology widely known up to now. These digital watermarking technologies have some advantages in that it is easy to embed watermark (spatial domain method) and it is difficult to remove watermark (frequency domain method), etc., whereas, they have various disadvantages in that it is weak in an operation like a filtering (spatial domain method), an image is damaged according to the value of coefficient (frequency domain method), or an original image is necessary for extracting watermark and an original image is largely altered by embedding watermark (spread spectrum communication method).

That is, the conventional digital watermarking technologies as described above failed to meet all the requirements, in particular, i) it must be difficult or impossible to remove the watermark embedded in a digital image (difficulty of access); ii) even if the digital image is printed or an image alteration for printing, for example, dithering or halftone, is made, the watermark embedded in the digital image must be robust enough to be extracted after such print or image alteration (robustness against alteration); iii) when watermark is embedded in the digital image, the deterioration of quality of the digital image by watermark must be minimized (conservation of quality of the digital image); and iv) the embedded watermark can not be known except a copyright holder or a person whose use is allowed (hiding of the embedded information) to prevent the illegal alteration, copy and distribution of the digital media thereby its range of

application is very restrictive and it is difficult to fully obtain the object described above.

SUMMARY OF THE INVENTION

5 Accordingly, it is an object of the present invention to provide a digital image watermarking technology that meets all the requirements as described above. More specifically, it is an object of the present invention to provide a digital image watermarking apparatus and method in that the extraction of the embedded watermark is possible despite of a print or various image alterations, 10 access to the watermark becomes difficult by embedding invisible watermark, and an original image is not necessary in extracting watermark.

15 It is another object of the present invention to provide a digital image watermarking apparatus and method wherein the quality of the digital image is not largely deteriorated and it is very strong in conserving the watermark when the digital image with watermark embedded is printed having high resolution or the image is altered due to dithering or halftone, etc. since a watermark is embedded using a frequency domain characteristic.

20 It is still another object of the present invention to provide a digital image watermarking apparatus and method in that user key value inputted by a user is encrypted and generated as watermark and then embedded, after extracting watermark from a digital image, by determining whether the watermark generated from a user key input from a user is the same as the watermark extracted, it must grant authentication only if two watermarks are same each other and thus the security of watermark is much intensified.

It is still another object of the present invention to provide a digital image watermarking apparatus and method that maximizes accuracy of a watermark extraction and authentication by using the sharpening filter, the fourth moment (Kurtosis), peak value and its location thereof in the correlation 5 between a user key value and watermark.

In order to achieve the object as described above, the present invention provides a method for embedding watermark into a digital image having a luminance component, comprising the steps of: (a) transforming said luminance component into coefficients of a frequency domain having a first frequency area and a second frequency area; (b) generating a replacement coefficient from a coefficient of said first frequency area and said watermark; (c) replacing a coefficient of said second frequency area with said replacement coefficient, whereby said watermark is embedded into said digital image; and (d) transforming said digital image embedded with said watermark into an inverse 10 frequency domain.

In order to achieve another object of the present invention, the present invention provides a method for authenticating the digital image, comprising the steps of: (e) transforming the luminance component of the digital image embedded with said watermark into the coefficients of the frequency domain; (f) generating 15 a watermark for authentication; (g) extracting said watermark embedded in said digital image by using the coefficients of said first and second frequency domains; and (h) authenticating said digital image by finding a correlation of said extracted watermark and said watermark for authentication.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram illustrating schematically the constitution of a watermark-embedding device according to the present invention.

5 Fig. 2 is a view illustrating a discrete wavelet transform process by a filter bank used in the present invention.

Fig. 3 is a view illustrating a discrete wavelet inverse transform process by a filter bank used in the present invention.

10 Fig. 4 is a view illustrating a general distribution of coefficients after a discrete wavelet transform used in the present invention.

Fig. 5 is a flow chart illustrating a process which embeds a watermark into a digital image according to the present invention.

Fig. 6 is a block diagram illustrating schematically the constitution of a watermark-authenticating device according to the present invention.

15 Fig. 7 is a flow chart illustrating a process that extracts a watermark from a digital image and outputs the authentication result from the computation and analysis of the correlation of the extracted watermark according to the present invention.

20 **DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS**

Hereinbelow, a digital image watermarking apparatus and method according to the preferred embodiment of the present invention referring to the figures attached are explained in detail.

In general, a digital image watermarking device is comprised of a digital image watermark embedding device for embedding watermark in a digital image and a digital image watermark authenticating device for authenticating image with watermark embedded. Such devices can be used in an independent or combination manner according to various embodiments.

5

10

First, referring to Fig. 1 and Fig. 5, a device and method that embed a watermark in a digital image are explained together. Fig. 1 is a block diagram illustrating schematically the constitution of a watermark embedding device according to the present invention and Fig. 5 is a flow chart illustrating a process which embeds a watermark in a digital image according to the present invention.

15

A series of process executed by a watermark embedding device 100 of Fig. 1 corresponds to a process illustrated in Fig. 5. Fig. 1 shows the constituents, which are included in a watermark embedding device 100 by function blocks, and Fig. 5 shows the proceedings executed by the constituents of Fig. 1.

20

First, an original image (OI) is inputted into a grey/color image discriminator 110 which is included in a watermark embedding device 100 (step 310). The grey/color image discriminator 110 is arranged forth to determine whether the original image (OI) for embedding a watermark is a grey image or a color image. The grey/color image discriminator 110 extracts image information data relating to input original image (OI) format, etc. and then discriminates whether it is a grey image or a color image from the extracted image information data (step 320).

Next, the original image (OI) which experiences the discriminating

process (step 320) by a grey/color image discriminator 110 is transformed to a frequency domain by a frequency domain transformer 125. At this time, since a grey image has only a luminance component, in the case the result by a grey/color image discriminator 110 is a grey image, only a frequency domain transform regarding the luminance component is executed and then at once a frequency transform by a frequency domain transformer 125 is executed (step 5 330a).

Differently from this, in the case the result in the discriminator 110 mentioned above is a color image, first in a color model transformer 120, for 10 example, a color model like RGB mode is transformed to a color model of HSB (H : hue, S : saturation, B : brightness) mode, YIQ (Y : luminance, I : in-phase, Q : quadrature) mode or YCbCr (Y : luminance, Cb/Cr : chrominance) mode, and the luminance component of the transformed color model is extracted (step 15 325). The luminance component of the color model transformed by a color model transformer 120 is transformed to a frequency domain by a frequency domain transformer 125 (step 330b).

There are many varieties of methods to transform the original image (OI) to the frequency domain in that, representatively, FFT (Fast Fourier Transform), DCT (Discrete Cosine Transform), DWT (Discrete Wavelet 20 Transform), etc. can be used.

The present invention uses the frequency domain method for embedding and extracting a watermark. That is why the frequency domain method has advantages that it makes removal of watermark difficult by hiding a watermark in the digital image and does not largely deteriorate quality of the original image.

In accordance with the frequency domain transformer 125, DCT coefficient, FFT coefficient or DWT coefficient (FOI) can be obtained.

Meanwhile, it is difficult in embedding watermark information in Fourier transform coefficient since in Fourier transform coefficients of the 5 transform domain comprise complex numbers, whereas DCT includes a characteristic similar to Fourier transform, but coefficients of the transform domain comprise real numbers. Hence, DCT is more advantageous and easier than Fourier transform. Hereinbelow it is explained as the embodiment that embeds watermark in the DCT coefficient or DWT coefficient regarding the 10 digital image. DCT is basically in a close relation with FFT and is a transform method widely used in the standard JPEG compression, etc.

The first dimensional DCT transform is defined as in the following equation 1a:

15 [Equation 1a]

$$t(k) = c(k) \sum_{n=0}^{N-1} s(n) \cos \frac{\pi(2n+1)k}{2N}$$

In the above equation 1a, s is an original signal value, t is a transformed signal value, N shows the length of signal, and coefficient c is as in the following 20 equation 1b:

[Equation 1b]

$$c(0) = \sqrt{1/N}, \quad c(k) = \sqrt{2/N}$$

(just in case of $1 \leq k \leq N-1$)

On the other hand, the second dimensional DCT regarding a square matrix is defined as in the following equation 2a:

[Equation 2a]

$$t(i, j) = c(i, j) \sum_{n=0}^{N-1} \sum_{m=0}^{N-1} s(m, n) \cos \frac{\pi(2m+1)i}{2N} \cos \frac{\pi(2n+1)j}{2N}$$

In the above equation 2a, N, s, and t have the same meaning as in the first dimensional DCT transform, $c(i, j)$ is as in the following equation 2b:

[Equation 2b]

$$c(0, j) = 1/N, \quad c(i, 0) = 1/N, \quad c(i, j) = 2/N$$

(just in case of $i \neq 0, j \neq 0$)

Further, the DCT has an inverse transform and is defined as the following equations 3a and 3b regarding each of the first and second dimensions:

[Equation 3a]

$$s(n) = \sum_{k=0}^{N-1} c(k) t(k) \cos \frac{\pi(2n+1)k}{2N}$$

[Equation 3b]

$$s(m, n) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} c(i, j) t(i, j) \cos \frac{\pi(2m+1)i}{2N} \cos \frac{\pi(2n+1)j}{2N}$$

Next, the DWT is reviewed. Fourier transform uses a sine function and cosine function as its basis function, whereas Wavelet transform uses wavelet as its basis function, which is divided into a continuous wavelet transform and discrete wavelet transform. The continuous wavelet transform is defined as in the following equation 4.

[Equation 4]

$$W(s, \tau) = \int_{-\infty}^{\infty} f(t) \psi(s, t) dt$$

In the above equation 4, s indicates scaling, τ indicates translation, $\psi(s, t)$ indicates wavelet which is scaled and translated.

The scaling is related to a frequency. A low scaling, i.e., the compressed wavelet extracts a high frequency component and a high scaling, i.e. the extended wavelet extracts a low frequency component. Usually, it is impossible to virtually realize the continuous wavelet transform since the wavelet coefficients obtained from the transform are infinite as a function of scaling and translation.

Hence, it can be more effectively realized if the discrete wavelet transform which selects only a certain frequency domain is used regarding the

scaling and translation. However, since the discrete wavelet transform also must stand a lot of computing amount to be realized by a computer, it is preferable to transform the image by using a fast wavelet transform of a filter bank. This method uses the conventional two channels of a sub-band coding and a pyramid algorithm and has advantage that it can be easily realized only if the relation PR-QMF (Perfectly reconstruction quadrature mirror filter) between filter banks for an inverse transform is carried out.

5 The abstract of the fast wavelet transform using filter bank is as shown in Fig. 2, Fig. 3, and Fig. 4. Fig. 2 illustrates the process of a discrete wavelet transform by a filter bank used in the present invention, Fig. 3 illustrates the process of a discrete wavelet inverse transform by a filter bank used in the present invention, and Fig. 4 illustrates a general distribution of coefficients 10 after a discrete wavelet transform used in the present invention.

15 Meanwhile, in accordance with the first embodiment of the present invention, in generating the watermark, a designated user key is inputted from authorized user, and the watermark is generated by the inputted user key. Should the user key is adopted as the watermark, via the correlation between the extracted watermark and the watermark generated from the user key, the 20 authenticity or any change made will be accurately determined. Thus, the present invention has an advantage that strengthens the security of the watermark.

Furthermore, in accordance with one embodiment of the present invention, after encrypting the inputted user key, a watermark to be embedded in the digital image is generated. If the user key undergoes the encryption

process, not only the value of the user key will not be easily transformed but also the user key itself can be hided. Thus, when the watermark generated from the encrypted user key is embedded in the digital image, the present invention has an advantage as the user key itself will not afterwards arise any concern for the user key itself to be reveled when extracting the watermark from the digital image.

The encryption may employ the conventional encryption methods, for example, data encryption standard (DES) method, RSA method, ECC method, etc. According to one embodiment of the present invention, as illustrated in Fig. 1, a PN-code method which outputs in pseudo random number the result of the coded data that will be encrypted is employed.

In order to generate the watermark (W), as illustrated in Figs. 1 & 5, should the user key be inputted in the watermark generator 130 (Step 341), the user key encryptor 131 and pseudo random number generator 132 included in the watermark generator 130 encrypt the user key using the inputted user key, generate pseudo random number (Steps 343 & 345), and generate watermark (W) which will be embedded in the frequency domain transform coefficient (FOI) of the original image (OI) (Step 340).

The watermark (W) generated from the user key is embedded in the digital image via a process such as the following equation 5 (Step 350a or Step 350b).

[Equation 5]

$$FOI' = f_x(|FOI|) \times W$$

wherein, f_x is a characteristic function for controlling the intensity of the watermark which will be embedded in the original image. f_x may be variously 5 set up which can be a function either performing an modulo operation of portion of the frequency domain transform coefficient (FOI) of the original image (OI) or rendering statistical values of the multiple transforming coefficients such as the mean, standard deviation, and variance etc.

FOI' represents the result of multiplying watermark (W) to a value 10 applying characteristic function f_x to the frequency domain transforming coefficient (FOI) of the original image (OI). The transform coefficient (FOI) in the above equation 5 is a value of the frequency domain of the digital image, therefore is in a two dimensional arrangement format. The watermark (W) has 15 one dimensional sequence format so that the transforming coefficient (FOI) is transformed into a sequence format or the watermark is transformed into a two dimensional block to perform the calculation. For performing the calculation, there is a method wherein per a frequency coefficient of the image, a watermark is matched thereto to calculate or a method wherein the statistical characteristics of various frequency coefficients of the image are selected to perform calculation 20 with a watermark.

To explain the process of embedding the watermark in more detail in reference to the equation 5, the watermark embedder (140) executes a process replacing a transform coefficient of another designated particular frequency

area with the result (FOI', hereinafter refer to as "replacement coefficient") of multiplying the value obtained from applying characteristic function f_x to the absolute value of the transform coefficient of the designated particular frequency area (hereinafter, refer to as "embedding coefficient") by watermark.

5 For example, when the digital image is divided into low frequency, middle frequency and high frequency areas, the watermark is embedded into the middle or high frequency areas containing relatively less digital image information. The watermark embedding is completed by replacing the transforming coefficient of the existing middle or high frequency areas with the 10 result (replacement coefficient) of multiplying the result from applying characteristic function f_x to the transform coefficient (embedding coefficient) of the low frequency area by watermark.

15 According to such method, eventhough there is a compressing process abandoning the high frequency portion or a transformation such as blurring, the watermark is multiplied by the coefficient of the low frequency area and replaced to the high frequency area, after the transformation, relatively large portion of the high frequency area remains. Thus, the present invention has an advantage of being robust to against the transformation.

The present specification sets forth the replacement of the watermark 20 multiplied by the result obtained from applying the characteristic function f_x to the absolute value of the coefficient of the low frequency area between to the areas the middle frequency and high frequency as an example. However, the watermark can be embedded by selecting a frequency area with range that does not degrade the quality of the digital image. For instance, as it is possible to

replace the watermark to the high frequency area after being multiplied by the result from applying the characteristic function to the absolute value of the transforming coefficient of the high frequency area, a method embedding the watermark in the digital image transformed to the frequency area is not limited thereto, but is also applicable to several frequency areas.

Also, should the present invention observing that the overall characteristics of the image is not easily changed from the print adopt the characteristics of the frequency domain which does not change the overall characteristics of the image by compensating the coefficient of the other frequency area with the arbitrary coefficient of the frequency area, it will become sturdy to the print. Thus, disappearance of the watermark at printing, etc. will be prevented. Furthermore, according to the watermark embedding method using the aforementioned characteristics of the frequency domain, as the overall characteristics of the digital image will not change even at the embedding 15 of the watermark, i.e. the quality of the original image is not degraded, it is possible to enjoy the quality of the original image even after being printed.

In equation 5, the intensity of the robustness of the watermark (W) when the watermark (W) is embedded in the original image (OI) is controlled by function f_x . Any value can become said characteristic function value since the 20 value can be set up by user as he pleases, and particularly, an appropriate function that does not degrade the quality of the digital image from embedding the watermark (W) can be determined. In other words, intensity of the robustness of the watermark is indirectly related with quality of the digital image or vice versa. Therefore, determination made in aspect of an

environment in which the watermark is used and a maintenance of the quality of the digital image is desirable.

Now, in order to acquire digital image embedded with watermark, an inverse frequency domain transformer (150) restores the transformed digital image. (Step 360a or Step 360b) When the aforementioned frequency domain transformer 125 employs discrete cosine transform (DCT) or discrete wavelet transform (DWT) or fast fourier transform (FFT), the inverse frequency domain transformer 150 employs inverse discrete cosine transform (IDCT) or inverse discrete wavelet transform (IDWT) or inverse fast fourier transform (IFFT). 5 At this point, when the original image (OI) is in color image, the color model of HSB mode, YIQ mode or YCbCr mode is restored by inverse color model transformer 155 to the original color model from employing the remaining constituent which did not undergo the frequency domain transformation and the luminance constituent wherein the inverse frequency domain transformation is 10 conducted (Step 370). Finally, by acquiring the digital image (WI) embedded with the watermark (Step 380), the embedding process of the watermark to the 15 digital image is completed.

Reffering to Fig. 6 and Fig. 7, the authentication result output device and method extracting watermark from the digital image embedded with watermark and via correlation between the extracted watermark and the watermark generated from the user key is explained below. 20

Fig. 6 is a block diagram illustrating schematically the constitution of the watermark authenticating device according to the present invention, and Fig. 7 is a flow chart illustrating the process of extracting watermark from the digital

image according to the present invention and outputting the authentication result from the computation and analysis of the correlation to the extracted watermark.

A series of process performed by the watermark authenticating device 200 of Fig. 6 corresponds to a process illustrated in Fig. 7. Fig. 6 depicts the constituent elements included in the watermark extraction and authentication device 200 in blocks according to their functions, and Fig. 7 depicts the extraction and authentication processes performed by the constituent elements of Fig. 6.

First, the digital image (WI) embedded with watermark is inputted into the grey/color image discriminator 210 of the watermark extraction and authentication device 200 (Step 410). The grey/color image discriminator 210, color model transformer 220, and frequency domain transformer 225 of Fig. 6 are identical to the grey/color image discriminator 110, color model transformer 120, and frequency domain transformer 125 of Fig. 1 in aspect of their operation and function.

In other words, the image (WI) embedded in the watermark is identified whether it is in grey image or in color image (Step 420), and should the image embedded in the watermark is in grey image, the frequency domain transform with regard to luminance constituent is conducted by frequency domain transformer 225 (Step 430a). If the image (WI) embedded in the watermark is in color image, first, the image is transformed to color model such as HSB mode, YIQ mode or YCbCr mode, etc. by color model transformer 220 (Step 425). Then, by frequency domain transformer 225, the frequency domain transform

such as discrete cosine transform (DCT) or discrete wavelet transform (DWT) or fast fourier transform (FFT) regarding luminance constituent is conducted (Step 430b).

As illustrated in Fig. 6 and Fig. 7, should the user key be inputted in the 5 watermark generator 230 (Step 441), the user key is encrypted by the user key encryptor 231 (Step 443) in the identical method as the watermark embedding process of Fig. 5, and watermark (W) according to PN-code method is generated by pseudo random number generator 232 (Step 445). The watermark generator 230 and the watermark generating process 440 of Fig. 6 and Fig. 7 are identical to the watermark generator 130 and the watermark generating process 10 340 of Fig. 1 and Fig. 5.

Next, the correlator 240 performs the inverse process of watermark embedding to extract watermark (WE) embedded in the digital image from the frequency domain transform coefficient (FWI) of the digital image embedded 15 with watermark obtained from the result of the frequency domain transform, and computes the correlation between the two watermarks (W and WE) (Step 450)

During watermark extraction, the process multiplying the result of applying the characteristic function to the coefficient of the designated 20 particular frequency area by the watermark and embedding into a coefficient of the other designated particular frequency area coefficient is inversely processed. From the digital image embedded with watermark, the replacement coefficient (FOI') embedded in the aforementioned particular frequency area and the embedding coefficient (FOI) used in the replacement coefficient (FOI')

calculation are obtained, and using these embedding coefficient and replacement coefficient, the watermark is restored. The correlation between the restored watermark (WE) and the watermark (W) generated by a method used in the watermark embedding is obtained so that it is possible to determine whether the 5 designated watermark is in the digital image.

Though it has not been illustrated in the drawings, other than the method generating the watermark from the user key, for example, there is an embodiment embedding and extracting any one of the various watermarks stored in advance in the designated storing medium. As such instance, when 10 the user key is not inputted, it is possible to determine whether the predetermined watermark is embedded by comparing the watermark obtained from the embedding coefficient and the replacement coefficient, for example, with the various watermarks stored in advance.

In any case, the watermark can be directly extracted from coefficient 15 values of the frequency domain of the image embedded with watermark, therefore the original image is not required.

Nevertheless, when the watermark has a sequence with arbitrary values, in order to restore the watermark, the embedding coefficient and the replacement coefficient values should be used. For example, if the watermark 20 contains binary sequence of only 1 and -1, the value of the watermark can be restored only by the signs of the replacement coefficient under the assumption that the value of characteristic function f_X is always positive.

The correlator 240 obtains the correlation between the watermark (WE) extracted as above and the watermark (W) generated by employing the key

inputted by the user and the correlation values thereof to confirm the watermark embedding designated by the user. Thus, it is possible to know by watermark extraction and authentication device 200 whether the digital image under inspection is authentic or altered.

5 The method to obtain the correlation between the two watermarks (WE and W) of the correlator 240 and the correlation values thereof is explained below.

The correlation between the two watermarks (WE and W) can be obtained from the following equation 6:

10 **[Equation 6]**

$$\text{Corr}(WE, W) = \sum_{k=0}^{N-1} WE \cdot W \equiv \text{real}(\text{IFFT}(\text{FFT}(WE) \times (\overline{\text{FFT}(W)} \times \text{FFT}(W))))$$

wherein, $\overline{\text{FFT}(W)}$ is a conjugate complex of $\text{FFT}(W)$, and $\text{IFFT}(W)$ represents an inverse $\text{FFT}(W)$.

15 The result of the correlation obtained from the above Mathematical Formula 6 is not a certain value, but is in a sequence form (X_1, \dots, X_N). Accordingly, the maximum peak value M and its position P are obtained in comparison of the obtained plurality numbers of values ($X_1 \sim X_N$).

20 Next, from the result of the correlation obtained from the following equation 6, the sharpness, i.e. the forth moment Kurtosis (K) is obtained from the equation 7.

[Equation 7]

$$Kurt(x_1, \dots, x_N) = \left\{ \frac{1}{N} \sum_{j=1}^N \left[\frac{x_j - \bar{x}}{\sigma} \right]^4 \right\} - 3$$

wherein, X_1, \dots, X_N is a sequence obtained from the above explained equation 6, and they are the resulting values of the correlation between two watermarks (W and WE). \bar{x} is the average of X_1, \dots, X_N and σ represents the standard deviation.

When analyzing the correlation values K, M and P obtained as above (Step 460), it is possible to determine whether the watermark (W) generated by the designated user key agrees to the watermark (WE) extracted. In more detail, when the correlation value K, i.e. Kurtosis is less than the predetermined threshold, the two watermarks (W and WE) do not agree to each other, and also when the maximum peak value (M) is less than the predetermined threshold, it represents that the two watermarks (W and WE) do not agree to each other. Furthermore, only when the position (P) of the maximum peak value of the two watermarks (W and WE) is always identical, it means that the two watermarks (W and WE) agree to each other. Moreover, PN-code generated by the watermark generator (230) has '0' correlation degree with PN-code excluding the signal of its own. Thus, when the correlation degree by PN-code is also the predetermined critical value or more, it means that the two watermarks (W and WE) are same each other. Accordingly, when the digital image satisfies all the requirements of the above-mentioned correlation values, it means that the two watermarks (W and WE) agree to each other so that the authentication of the

digital image can be confirmed. For instance, a person in possession of a certificate printed with a digital image watermarked in accordance with the result analyzing the requirements of the correlation values such as Step 370 of Fig. 7 is either authenticated or for example, is permitted his pass (Step 480a), or 5 is rejected of the authentication, for example, is refused his pass or is given a warning (Step 480b).

In order to evaluate the digital watermarking device and method according to the present invention; an experiment extracting the watermark after embedded with the digital image of size 256 X 256 and then inflicting 10 transformation such as dithering, halftone, and blurring etc. is conducted. With regard to this experiment, the extraction result of approximately 99.92% is obtained. The experiment is continuously conducted to extract watermark after the image printed from a printer in a resolution of 300dpi is generated again into the digital image using a scanner and a digital camera. This 15 experiment showed a high extraction rate of more than 95%. Hence, it has been proved that the present invention has a watermarking technique powerful against the transformation due from being printed.

As described above, according to the digital image watermarking apparatus and method of the present invention, the principle of the present 20 invention using the characteristic of the frequency domain provides such advantages that the quality of original image is guaranteed against embedment and extraction of watermark, and the watermark that is resistant to printing or image transform can be extracted without using the original image. Also, the security and accuracy of watermark are significantly strengthened by

embedding watermark generated from a user key, authenticating a digital image only when watermark generated from the user key inputted by a user is consistent with the watermark as extracted when extracting watermark, and using the correlation value such as the 4th moment (Kurtosis).

5. The apparatus and method of the present invention, being resistant to the printing and providing the enhanced security, are applicable to various applied examples requiring a copyright or authentication as printed matters and confirmation of personal information. That is, it is provided an information security device and method thereof as preconditions for activating electronic commerce, an electronic certificate of authentication, an electronic identification card, an electronic registration, an internet coupon, electronic cash, an identification card, a school record and the like on large-scale network such as internet. Also, since it is possible to prevent illegal transformation or use such as forgery and alteration of information needed for secrete maintenance, the 10 present invention can be widely applied to the intellectual property protection industry field of copyrighted digital image materials as well as protection of personal information.

15. Although the preferred embodiments of the digital image watermarking apparatus and method according to the present invention are disclosed for illustrative purposes, it will be obvious to those skilled in the art that such embodiments are merely for illustrations but are not restricted to the illustrations themselves, and can be variously changed, transformed and replaced within the scope of the technical idea of the present invention. Further, it should be understood that the technical idea of the present invention

is not restricted to the aforementioned embodiments but to only the claims attached hereto and their equivalent technical principle.

What is claimed is :

1. A method for embedding watermark into a digital image having a luminance component, comprising the steps of:

- 5 (a) transforming said luminance component into coefficients of a frequency domain having a first frequency area and a second frequency area;
- (b) generating a replacement coefficient from a coefficient of said first frequency area and said watermark;
- (c) replacing a coefficient of said second frequency area with said 10 replacement coefficient, whereby said watermark is embedded into said digital image; and
- (d) transforming said digital image embedded with said watermark into an inverse frequency domain.

15 2. The method according to claim 1, wherein said digital image is a color image and said method further comprises the steps of:

- before said step (a),
 - (a') transforming said digital image into a color model including the luminance component and extracting the luminance component of said 20 transformed color model; and
- after said step (d),
 - (d') performing a color model inverse transform of said digital image as transformed into said inverse frequency domain by using the luminance component for which said inverse frequency domain transform is performed,

and the remaining components with the exception of said luminance component for which said frequency domain transform is not performed.

3. The method according to claim 2, wherein said color model including said luminance component is one of HSB mode, YIQ mode and YCbCr mode.

4. The method according to claim 1, wherein said replacement coefficient is generated in such manner that said watermark is multiplied by the operation result obtained by applying a predetermined characteristic function to an absolute value of the coefficient of said first frequency area.

5. The method according to claim 4, wherein said first frequency area is a low frequency area and said second frequency area is between a middle frequency area and a high frequency area.

6. The method according to claim 4, wherein said characteristic function is the modulo operation result of parts of said frequency domain transform coefficients, or a function represents the statistical characteristic of said frequency domain transform coefficients.

7. The method according to claim 1, wherein said step (a) uses one of among FFT, DCT, and DWT.

8. The method according to claim 1, wherein said watermark is generated by

encrypting a user key and generating pseudo random number from said encrypted user key.

9. The method according to claim 8, wherein said encryption is executed by PN-
5 code method.

10. A method for authenticating the digital image by extracting watermark from the digital image embedded with watermark by the method of any one of claims 1 to 9, the method comprising the steps of:

10 (e) transforming the luminance component of the digital image embedded with said watermark into the coefficients of the frequency domain;

(f) generating a watermark for authentication;

(g) extracting said watermark embedded in said digital image by using the coefficients of said first and second frequency domains; and

15 (h) authenticating said digital image by finding a correlation of said extracted watermark and said watermark for authentication.

11. The method according to claim 10, wherein said watermark for authentication is generated by encrypting a user key and generating pseudo random number from said encrypted user key.

20 12. The method according to claim 10, wherein said step (h) comprises the steps of:

(h1) finding the maximum peak value and the position of said maximum

peak value from the correlation between said extracted watermark and said watermark for authentication;

(h2) finding the 4th moment from said correlation;

(h3) judging that said extracted watermark is same with said watermark for authentication in case where said 4th moment is over the predetermined critical value, the maximum peak value of said correlation is over the predetermined critical value, and the position of the maximum peak value of said correlation is the same.

10 13. The method according to claim 10, wherein said step (h) comprises the step of:

in case where said user key is encoded in PN-code method during the embedding process of said watermark, judging the consistency of said extracted watermark and said watermark for authentication when the correlation by said PN-code method is over the predetermined critical value.

14. An apparatus for embedding a watermark into a digital image having a luminance component, comprising:

frequency domain transform means for transforming said luminance component into coefficients of a frequency domain having a first frequency area and a second frequency area;

watermark generating means for generating said watermark;

replacement coefficient generating means for generating a replacement coefficient from a coefficient of said first frequency area and said watermark;

replacing means for replacing a coefficient of said second frequency area with said replacement coefficient, whereby said watermark is embedded into said digital image; and

5 inverse frequency domain transform means for transforming said digital image embedded with said watermark into an inverse frequency domain.

15. The apparatus according to claim 14, further comprising:

discriminating means for discriminating whether said digital image is a grey image or a color image;

10 in case where said digital image is the color image, the apparatus further comprising:

color model transform means for transforming said digital image to a color model including the luminance component and extracting the luminance component of said transformed color model to provide said frequency domain transform means; and

15 inverse color model transform means for performing a color model inverse transform of said digital image transformed from said inverse frequency domain transform means, by using the luminance components for which said inverse frequency domain transform is performed, and the remaining components with the exception of said luminance components for which said frequency domain transform is not conformed.

20 16. The apparatus according to claim 14 or 15, wherein said watermark generating means comprises:

encrypting means for encrypting a user key; and
pseudo random number generating means for generating pseudo
random number from said encrypted user key.

5 17. An apparatus for authenticating the digital image embedded with watermark
at the digital image watermark embedding apparatus of claim 15, the apparatus
comprising:

frequency domain transform means for transforming the luminance
component of the digital image embedded with said watermark into coefficients
10 of the frequency domain;

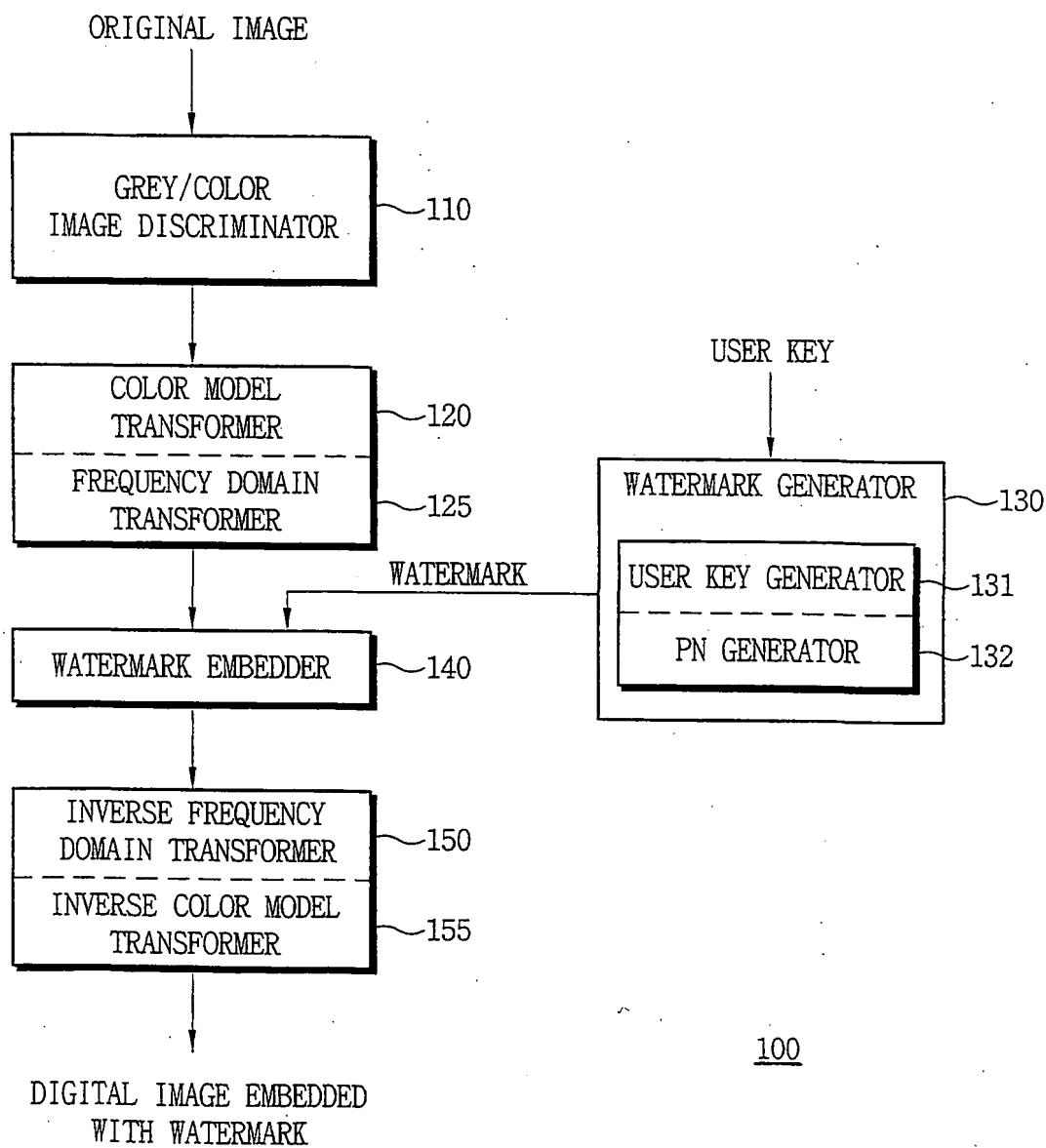
watermark generating means for generating watermark for
authentication;

watermark extracting means for extracting said watermark embedded
into said digital image by using the coefficients of said first and second frequency
15 domains; and

correlation computation means for authenticating said digital image by
finding a correlation between said extracted watermark and said watermark for
authentication.

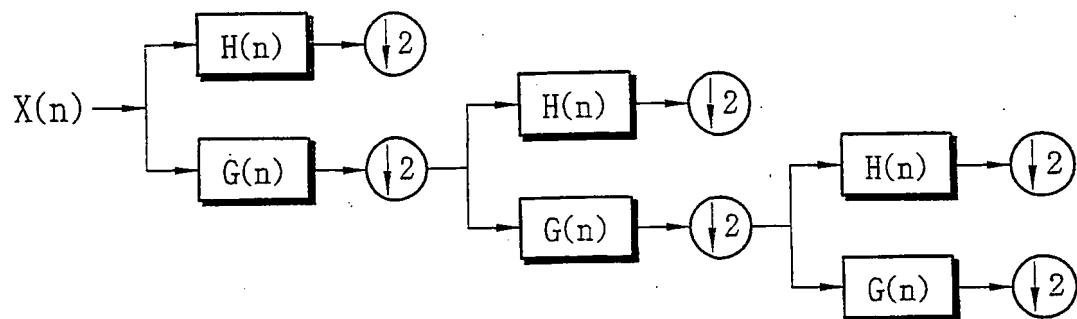
1/5

FIG. 1



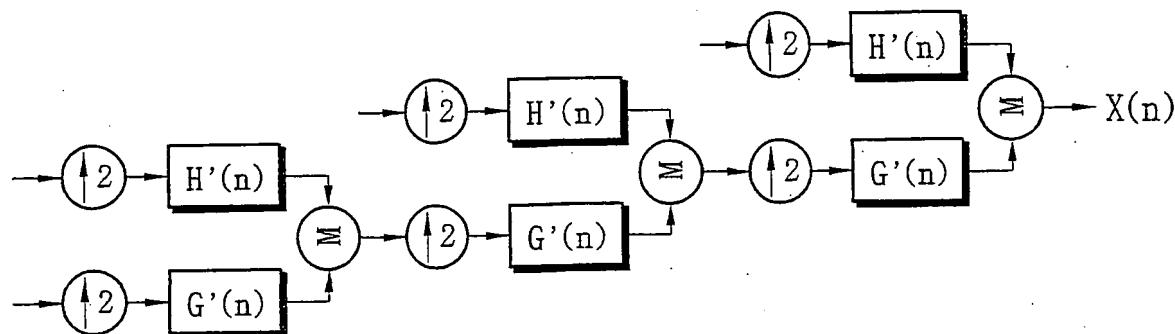
2/5

FIG. 2



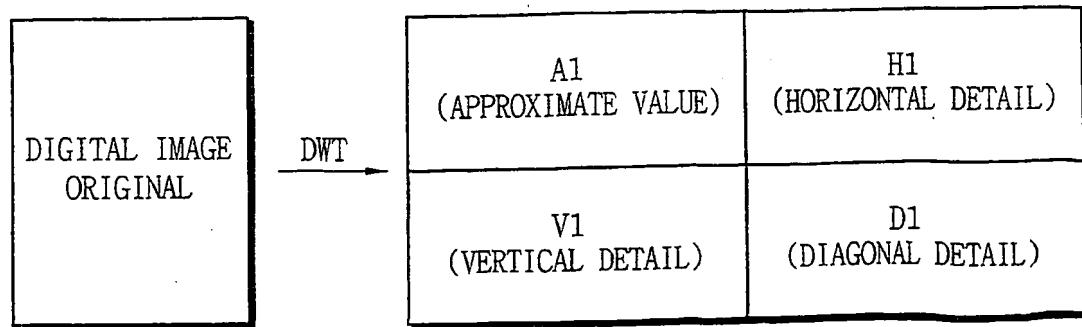
DISCRETE WAVELET TRANSFORM BY A FILTER BANK

FIG. 3



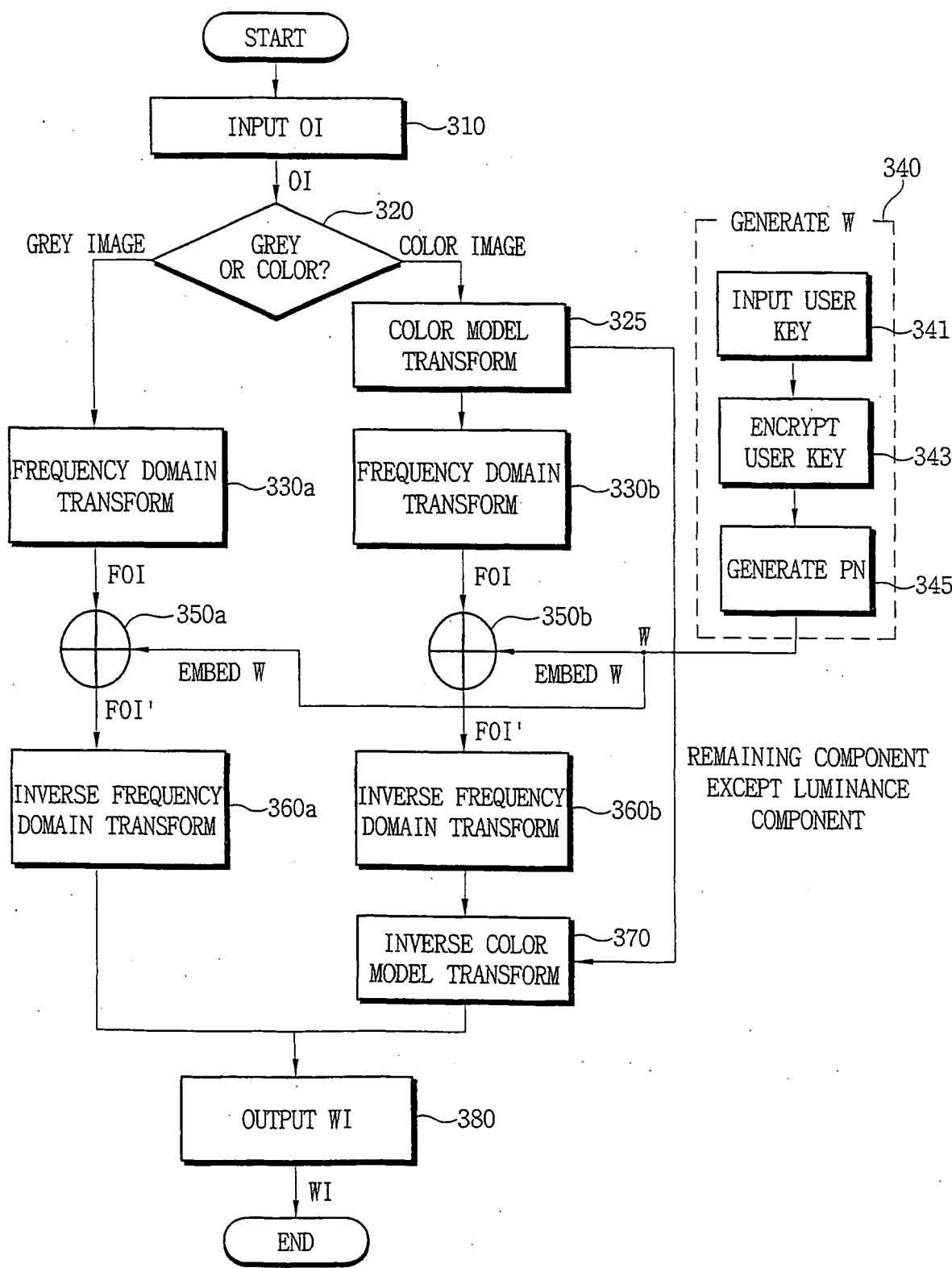
INVERSE DISCRETE WAVELET TRANSFORM BY A FILTER BANK

FIG. 4



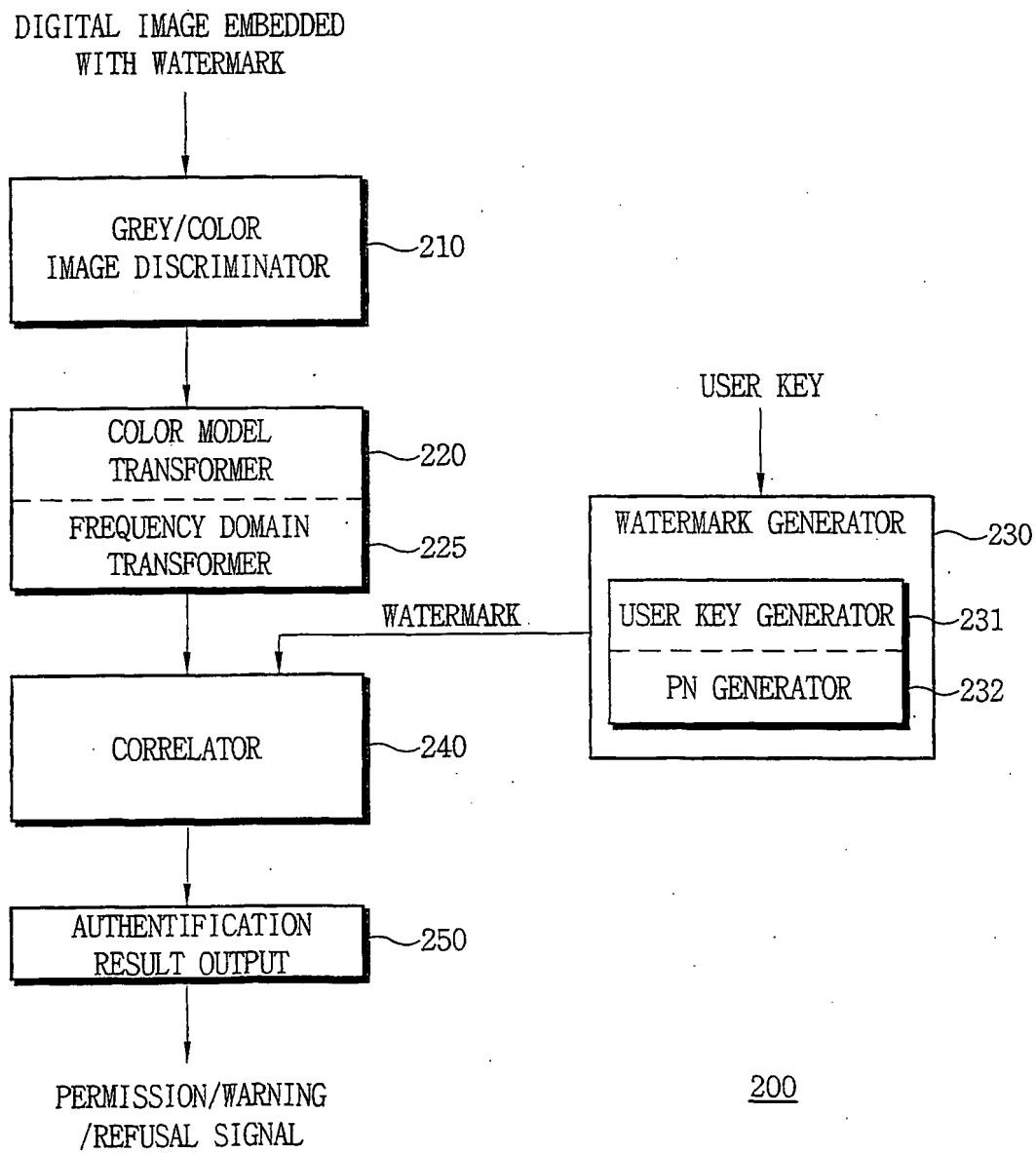
3/5

FIG. 5

REMAINING COMPONENT
EXCEPT LUMINANCE
COMPONENT

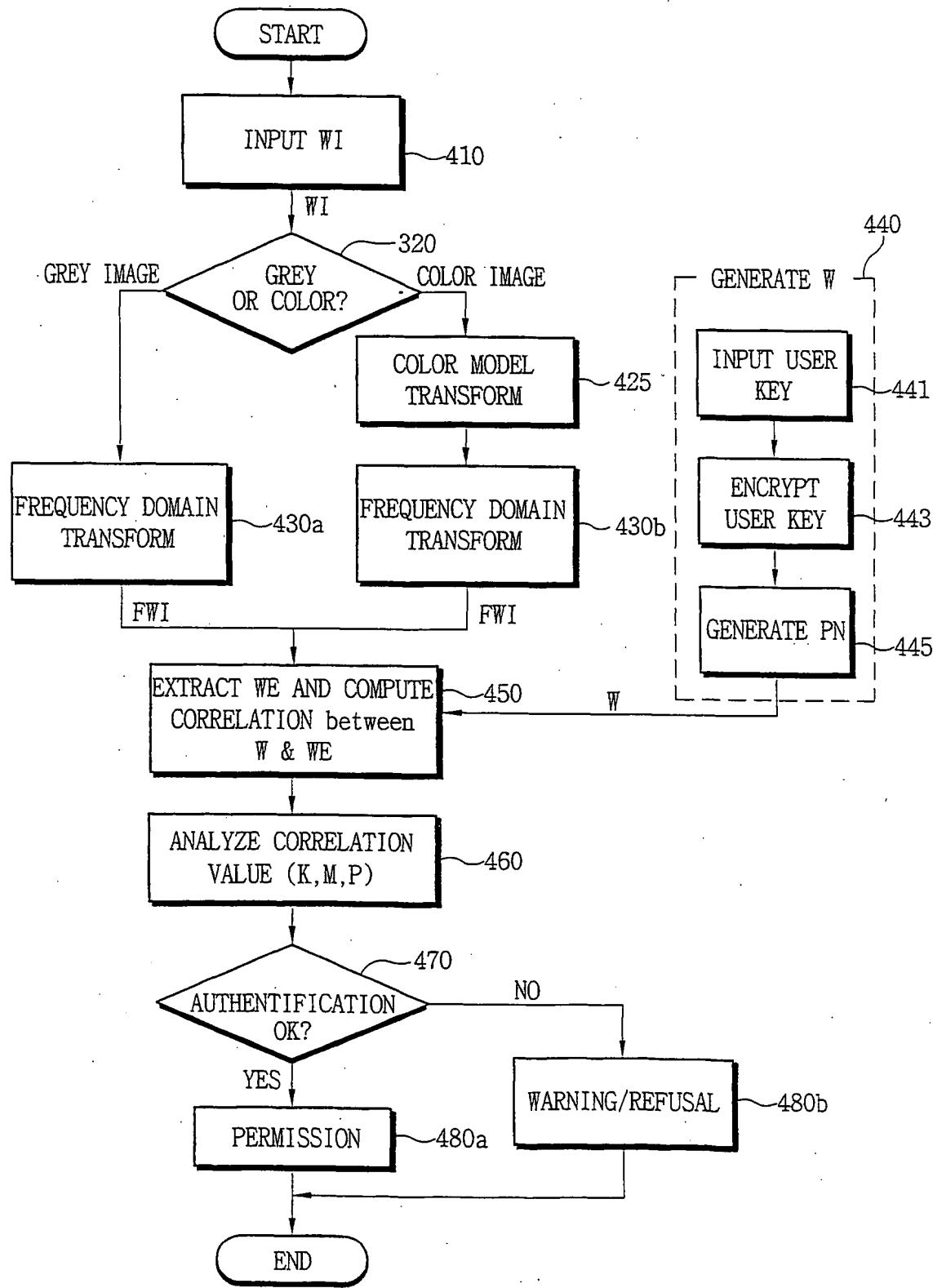
4/5

FIG. 6



5/5

FIG. 7



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR01/01524

A. CLASSIFICATION OF SUBJECT MATTER

IPC7 H04N 7/24

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

HO4N 1/387, 1/32, 7/167, 7/24, ; G06T 1/00; G11B 20/10;

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

KR, JP, EP: classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
E, A	EP1148708 A (KOWA CO) 2001-10-24	1- 17
A	EP1006710 A (TOKYO SHIBAURA ELECTRIC CO) 2000-06-07	1- 17
A	EP0891071 A(MATSUSHITA ELECTRIC IND CO LTD) 1999-01-13	1-17
A	US5809139 A (VIVO SOFTWARE INC) 1998-09-15	1-17
A	JP 11032200 A (MATSUSHITA ELECTRIC IND CO LTD) 1999-02-02	1-17

 Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier application or patent but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
24 JANUARY 2002 (24.01.2002)Date of mailing of the international search report
25 JANUARY 2002 (25.01.2002)Name and mailing address of the ISA/KR
Korean Intellectual Property Office
Government Complex-Daejeon, 920 Dunsan-dong, Seo-gu,
Daejeon Metropolitan City 302-701, Republic of Korea
Facsimile No. 82-42-472-7140Authorized officer
CHO, Kwang Hyun
Telephone No. 82-42-481-5987